REMARKS

The present amendment is in response to the Office Action dated February 27, 2007. Claims 1-5, 7-14, 23-30, and 32-43 are now present in this case. Claims 1, 23, and 30 are amended.

The Examiner will kindly note that representation in this matter has been transferred to another attorney. A revocation/substitute power of attorney is enclosed herewith.

Claim 1, stand rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement. The applicant respectfully traverses this rejection and request reconsideration. The applicant has amended claim 1 to more clearly recite the nature of the invention. The invention as presently claimed is clearly supported by the specification at page 2, lines 15-25. Accordingly, the applicant respectfully requests that the Examiner withdraw the rejection of claim 1 under 35 U.S.C. § 112, first paragraph.

Claims 30, 32-35, and 38 stand rejected under 35 U.S.C. § 103(a) as unpatentable by U.S. Patent No. 6,735,702 to Yavatkar et al. The applicant respectfully traverses this rejection and request reconsideration. Yavatkar is directed to a distributed system for diagnosing network intrusion. Yavatkar describes two types of agents. A watchdog agent is fixed in position at selected network nodes to detect a network attack and to create a second agent type, a bloodhound agent, which analyzes attack traffic by "moving through the network and gathering information" while the watchdog agent remains stationary." (See column 3, lines 46-54.) Thus, Yavatkar discloses a distributed system in which a number of watchdog agents are fixed in position throughout the network and perform monitor functions. When an intrusion is detected, one or more of the distributed watchdog agents activates and releases bloodhound agents that travel throughout the system to gather information.

While Yavatkar is directed to network security, it accomplishes the task in a fundamentally different way than that recited in claim 30. Specifically, claim 30 is directed to a central server and recites *inter alia* "receiving notification of a network intrusion at a central server." Claim 30 further recites "transmitting an intrusion

detection software installation request from the central server to a plurality of remote computers in response to the notification." Yavatkar teaches away from a central system by installing watchdog software at a plurality of nodes on a network. (See, e.g., column 3, lines 49-50.) When one of the watchdog agents distributed throughout the network detects an intrusion, it releases the mobile bloodhound agents to trace and track the intrusion. Thus, Yavatkar discloses a distributed detection system and teaches directly away from the central system recited in claim 30. For at least this reason, claim 30 is allowable over Yavatkar.

Furthermore, claim 30 recites transmitting an installation request from the central server to a plurality of remote computers in response to the notification and installing intrusion detection software on the plurality of remote computers via a software agent program in response to the request. (Emphasis added.) The Office Action asserts that the mere launching of agents or installing intermediate filters in the network meets the recitation of transmitting the installation request. The applicant respectfully disagrees. Yavatkar describes releasing the mobile agents in response to detecting software, but does not teach or suggest transmitting an installation request to remote computers and only installing installation software on the remote computers in response to the request. Yavatkar merely describes releasing the mobile agents for installation. There is no two-step process of requesting installation and installation in response to the request, as recited in claim 30. Yavatkar does not teach or suggest such a two-step process. Accordingly, claim 30 is allowable over Yavatkar. Claims 32-38 are also allowable in view of the fact that they depend from claim 30, and further in view of the recitation in each of those claims.

Claims 1-4, 7-10, 13-14, 23-25, and 27-29 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Yavatkar et al., combined with U.S. Patent No. 6,842,781 to Lavian et al. The applicant respectfully traverses this rejection and request reconsideration. As discussed above, Yavatkar is directed to a distributed system in which distributed watchdog agents monitor activity and, upon the detection of a network intrusion, send roaming bloodhound agents to trace attack traffic on the network and to analyze paths taken by the traffic. (See column 16, lines 25-29.) The roaming bloodhound agents are not directed by any central location or a human operator and

operate autonomously to determine which pathway to take throughout a network. (See column 4, lines 30-34.) Thus, there is no central server in Yavatkar that directs the operation of the mobile agents. The mobile agents act on their own. In sharp contrast to Yavatkar, claim 1 is directed to a method that recites *inter alia* "receiving a request from a central server at a software agent program installed on each of a plurality of remote computers to initiate intrusion detection services on each respective one of the plurality of remote computers." Yavatkar teaches directly away from this concept because the mobile agents are not directed by a central server and thus receive no request to initiate intrusion detection surfaces. Indeed, the very concept of Yavatkar is a distributed system wherein the mobile bloodhound agents determine, without direction from a central server, which computer on the network they should relocate to while tracing the network attack. Thus, Yavatkar adopts an entirely different approach than the method recited at claim 1.

The Office Action acknowledges that Yavatkar is silent about the request being received from a server and cites Lavian as describing a system for performing network management. The applicant notes at the outset that Lavian is directed to a totally different technology and is classified by the U. S. Patent Office an entirely different classes and subclasses with no overlap between the classification or fields of search between Yavatkar and Lavian. One skilled in the art is unlikely to combine two such disparate references in the manner suggested in the Office Action.

Even if one considers Lavian to be analogous art, the combination of the network server and Lavian is entirely incompatible with the distributed non-centralized approach described in Yavatkar. Yavatkar describes the autonomous operation of the mobile bloodhound agents as advantageous "because communication between a central console and a remote node is not required and thus a finer granularity of information can be collected and acted upon." (See column 4, lines 30-35.) Thus, the combination suggested in the Office Action is non-functional and attempts to combine to incompatible systems. The combination of references do not suggest software agents installed on a plurality of remote computers that receive a request from a central server to initiate intrusion detection services on each respective one of the plurality of remote computers, as recited in claim 1. For at least this reason, claim 1 is allowable over the

combination of Yavatkar and Lavian. Claims 2-5, 7-14, and 39-43 are also allowable in view of the fact that they depend from claim 1, and further in view of the recitation in each of those claims.

With respect to claim 23, Yavatkar discloses a distributed system described in detail above. In the system of Yavatkar, the mobile bloodhound agents operate autonomously and determine on their own which computer to relocate to in order to trace an intrusion throughout the network. Nothing in Yavatkar suggests that these plurality of computers are executing any software prior to the arrival of the mobile bloodhound agent. The mobile bloodhound agent arrives after an intrusion has been detected. (See column 3, lines 47-54.) In contrast, claim 23 recites "a plurality of computers executing software agents." Yavatkar does not describe computers executing software agents. Although the mobile bloodhound agents do move from computer to computer, they do so after detection of a network intrusion. Claim 23 further recites an intrusion detection server configured to "send a request to install and execute intrusion detection software to software agents at the plurality of computers when intrusion detection services are needed." Thus, the software agents are executing on the plurality of computers prior to the point in time when intrusion detection services are needed. This is in contrast to Yavatkar where the mobile bloodhound agents are sent to a plurality of computers after detection of an intrusion. The system of claim 23 sends a request to install the detection software to the software agents already executing at the plurality of computers whereas the system of Yavatkar only delivers the agents to the computers only after an intrusion is detected. Thus, Yavatkar does not teach or suggest the system of claim 23 wherein computers are executing software agents wherein the software agents receive a request to install and execute intrusion detection software.

The Office Action recognizes that Yavatkar does not suggest a server and cites Lavian as describing a server for network management. The inapplicability and distinct patent classifications of these two references has already been discussed above. Furthermore, as previously discussed, the combination proposed in the Office Action is non-functional. The very concept of central server operation in Lavian is incompatible with the non-centralized autonomous bloodhound agents described in

Yavatkar. Furthermore, even the combination of references does not suggest the system of claim 23 wherein software agents are already executing on a plurality of computers and respond to a request from a server to install intrusion detection software. Nothing in these references suggests software agents that are executing on the plurality of computers when they receive a request for installation of intrusion detection software. Thus, claim 23 is allowable over the combination of Yavatkar and Lavian. Claims 24-29 are also allowable in view of the fact that they depend from claim 23, and further in view of the recitation in each of those claims.

Claims 5, 11, 12, and 41-43 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Yvatkar et al., Lavian et al. combined with U.S. Patent Publication No. 2002/0003884 to Sprunk. The applicant respectfully traverses this rejection and request reconsideration. The inapplicability of the combination of Yavatkar and Lavian has already been discussed in great detail above. Those arguments need not be repeated herein. The Office Action cites Sprunk as describing techniques for halting operation of intrusion detection services. However, the combination of Yavatkar, Lavian, and Sprunk do not teach the method of claim 1 or the further details of dependent claims rejected herein. Specifically, it is noted that Sprunk is directed to techniques for authorizing video download files. While Sprunk recognizes that computers are susceptible to viruses and hackers, this is different from a network attack. Sprunk is only concerned with preventing a virus within a particular computer to prevent unauthorized access to the video file downloaded to that computer. This is significantly different from a network intrusion. Furthermore, Sprunk does not suggest any software agents or intrusion software installed on the plurality of remote computers. In short, Sprunk is directed to entirely different technology and is unrelated to the present application. Claim 1 is allowable for the reasons discussed above. Dependent claims 5, 11, 12, and 41-43 are also allowable in view of the fact that they depend from claim 1, and further in view of the recitation in each of those claims.

Claims 36-37 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of Yvatkar et al. and Sprunk. The applicant respectfully traverses this rejection and request reconsideration. The inapplicability of Yavatkar to the claimed invention has already been discussed above. Specifically, Yavatkar discloses a system

in which bloodhound agents move from one node to another autonomously. There is no teaching or suggestion in Yavatkar of transmitting an installation request from a central server to the remote computers and installing intrusion detection software via a software agent program on the computer in response to the request. The mobile bloodhound agents of Yavatkar act autonomously and not under the control of any central server. The addition of Sprunk does not overcome this serious shortcoming. The combination of Yavatkar and Sprung do not teach or suggest the notification and request process from a central server, as recited in claim 30. Thus, claim 30 is allowable for the reasons discussed above. Dependent claims 36-37 are allowable in view of the fact that they depend from claim 30, and further in view of the recitation in each of those claims. The Office Action interprets Yavatkar as disclosing a stop condition. The applicant respectfully disagrees with this assessment. The so-called stop condition referred to in the Office Action is not a stop condition "indicating when to stop executing the intrusion detection software," as recited in claim 36. Rather, the distributed mechanisms discussed in Yavatkar allow a mobile agent to trace an attack throughout the network. This requires the mobility of the bloodhound agent, which moves from one node to another. The fact that a mobile bloodhound agent ceases activity on one node in order to relocate to another node does not mean that the intrusion detection software has halted. Instead, the intrusion detection software has merely moved to another location in order to continue its operation.

Furthermore, the Office Action asserts that Sprunk discloses that a stop condition is an expiration time. However, the so-called expiration time in Sprunk is merely the time at which authorization for use of the downloaded video has expired. In effect, the so-called intrusion detection software of Sprunk is activated upon expiration of a certain time period so that the downloaded video file is disabled. If there is a software agent anywhere in Sprunk, it is activated upon a time expiration so as to disable the downloaded video file. In contrast, the stop condition recited in claim 37 is a stop condition at which the intrusion detection software stops executing. Thus, claims 36 and 37 are allowable over the combination of Yavatkar and Sprunk.

Claims 26 and 39-40 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Yvatkar et al., Lavian et al. combined with U.S. Patent No. U.S.

Patent No. 6,401,238 to Brown et al. The applicant respectfully traverses this rejection and request reconsideration. The inapplicability of the combination of Yavatkar and Lavian has already been discussed in great detail above. Specifically, the two references are totally incompatible in that Lavian is alleged to disclose central server operation while Yavatkar describes the undesirability of such centralized control and describes a distributed system in which mobile bloodhound agents operate autonomously. Thus, the combination of references is inoperable. Brown is cited in the Office Action as disclosing a deployment of applications based on time of day. However, Brown is unrelated to any intrusion detection technology. The use of time of day in Brown is merely to accommodate bandwidth limitations in a network that may be based on time of day. However, Brown is totally devoid of discussion of the plurality of computers executing software agents and installing executing intrusion detection software based on the time of day. The simple fact that network load balancing may be based on time of day is an insufficient basis for reaching the conclusion that intrusion detection software is activated or deactivated based on the time of day. Thus, claims 26, 39, and 40 are allowable over the combination of Yavatkar, Lavian, and Brown.

In view of the above amendments and remarks, reconsideration of the subject application and its allowance are kindly requested. The applicant has made a good faith effort to place all claims in condition for allowance. If questions remain regarding the present application, the Examiner is invited to contact the undersigned at (206) 757-8029.

Respectfully submitted,
Arturo Maria
Davis Wright Tremaine LLP

/Michael J. Donohue, Reg. #35859/

Michael J. Donohue

MJD:gatc
1201 Third Avenue
Suite 2200
Seattle, Washington 98101
Phone: (206) 757-8029
Fax: (206) 757-7029
2014460_1.DOC